Defense API

Smart LabsAI

Schützt LLMs vor Angriffen – stoppt Exfiltration

Unternehmen integrieren KI immer tiefer in ihre Prozesse, was neue Sicherheitsrisiken mit sich bringt. Ohne angemessenen Schutz werden KI-Systeme zu einer kritischen Schwachstelle.

Warum KI-Sicherheit kritisch ist

Jeder 4. Angriff auf aktuelle KI-Modelle hat Erfolg.

Ohne angemessenen Schutz werden KI-Systeme zu einer kritischen Schwachstelle.

Jeder Angriff birgt die Gefahr von **Datenexfiltration**

Damit können Konkurrenten sie im Wettbewerb ausstechen

Machen Sie ihre KI DSGVO konform

Filtern ihre Mitarbeiter aktuell personenbezogene Daten bevor Sie die KI suchen lassen?

Ihre Vorteile mit Defense API

Schützen Sie Ihre KI vor Manipulation

Überwachen Sie Ihre KI-Agenten in Echtzeit

Sichern Sie Ihre KI innerhalb von 10 Minuten ab!